Privacy, Security and Trust in the Internet of Neurons

Diego Sempreboni
Department of Informatics
King's College London, UK
diego.sempreboni@kcl.ac.uk

Luca Viganò
Department of Informatics
King's College London, UK
luca.vigano@kcl.ac.uk

***Abstract*—Arpanet, Internet, Internet of Services, Internet of Things, Internet of Skills. What next? We conjecture that in 15-20 years from now (which puts us more or less in the timeframe of some of the episodes of the Black Mirror anthology television series), we will have the Internet of Neurons, a new Internet paradigm in which humans will be able to connect bi-directionally to the net using only their brain. The Internet of Neurons will provide new, tremendous opportunities thanks to constant access to unlimited information. It will empower all those outside of the technical industry, actually it will empower all human beings, to access and use technological products and services as everybody will be able to connect, even without possessing a laptop, a tablet or a smartphone. The Internet of Neurons will thus ultimately complete the currently still immature democratization of knowledge and technology. But it will also bring along several enormous challenges, especially concerning security (as well as privacy and trust).**

In this paper we speculate on the forthcoming worldwide deployment of the Internet of Neurons and brainstorm about its disruptive impact, discussing the main technological (and neurological) breakthroughs required to enable it, the new opportunities it provides and the security challenges it raises. We also elaborate on the novel system models, threat models and security properties that are required to reason about privacy, security and trust in the Internet of Neurons.

I. Introduction: from the human computer to... the human computer

We all carry around a computer, regardless of who we are, how old we are, where we live, what job we do, what education we received. No, we are not talking about your laptop, your tablet or your smartphone. We are talking about your *brain*.

In fact, the term "computer" has been in use from the early 17^{th} century, way before electronic computers became available. It was introduced simply to mean "one who computes", namely a person whose job is to perform complex mathematical calculations. In that sense, people often speak of "human computer" to make this distinction clear.[1] Throughout the centuries, human computers, working alone or in teams, have provided significant contributions to groundbreaking scientific discoveries, ranging from trigonometry to astronomy, to the dawn of nuclear energy and nuclear weapons (e.g., the complex computations crucially related to nuclear fission in the Manhattan Project) and to the space race [2].

[1]In [1], Turing wrote: "The human computer is supposed to be following fixed rules; he has no authority to deviate from them in any detail."

When electronic computers became available in the second half of the 20^{th} century, human computers became useless, and "human computer" is nowadays mainly used to refer to individuals with prodigious powers of mental arithmetic who display their abilities in theaters or TV shows. Electronic computers also brought along a revolution that has transformed the economic, social, educational, and political landscape in a profound and indelible manner: the *net*.

The technical foundations of the Internet were laid by the Advanced Research Projects Agency Network *ARPANET* [3] towards the end of the 1960s. Soon after, new overseas nodes of the network were created and the definition of the standard TCP/IP officially launched the *Internet* as a set of interconnected networks through these packet switching protocols.

Advances in hardware and software at the end of the 20^{th} century enabled mobile connectivity to billions of laptops and (smart)phones. This *Mobile Internet* gave rise to the *Internet of Services (IoS)* [4], [5], with the flourishing of e-commerce, health-care portals, booking services, streaming websites and, last but not least, social networks. This redefined entire segments of the economy in the first decade of the 21^{st} century, and was soon followed by the *Internet of Things (IoT)*, a network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data [5], [6], [7], [8].

The next, and 5^{th}, evolution of the Internet is expected to be the *Tactile Internet*, which has been defined by the International Telecommunication Union (ITU) as a network that is based on 5G and combines ultra-low latency with extremely high availability, reliability and security [9], [10]. The Tactile Internet will encompass human-to-machine and machine-to-machine interaction, enabling tactile and haptic sensations and the control of the IoT in real time. It will unleash the full potential of the fourth industrial revolution (a.k.a. Industry 4.0), and revolutionize the way we learn and work through the *Internet of Skills* (a.k.a. Human 4.0, [11]). Although 5G has long passed the embryonic stage, and the testing phase is now underway, extra work is needed to tackle 5G security challenges [12], [13] in order to consider 5G a fully adoptable technology. However, capitalizing on 5G and ultra-low delay networking as well as on AI and robotics, the Internet of Skills will enable the real-time delivery of skills in

digital form remotely and globally.

After this brief overview of the past, and the near future, of the Internet, it is time to ask what will came next. We conjecture the return of the human computer, but in a different guise. We predict the coming of the next, and maybe ultimate, phase of the Internet evolution: the *Internet of Neurons* will rest upon a novel paradigm in which humans are able to connect bi-directionally to the net using only their brain. The Internet of Neurons will provide new, tremendous opportunities thanks to constant access to unlimited information. It will empower all those outside of the technical industry, actually it will empower all human beings, to access and use technological products and services as everybody will be able to connect, even without possessing a laptop, a tablet or a smartphone. The Internet of Neurons will thus ultimately complete the currently still immature democratization of knowledge and technology. It will also suggest a diversity of plots for new episodes of Black Mirror; in fact, as we will discuss below, some of the aired episodes already contain glimpses of some of the possible features of the Internet of Neurons. But, more importantly, the Internet of Neurons will also bring along several enormous challenges, especially concerning privacy, security and trust.

In the rest of this paper, we speculate on the forthcoming worldwide deployment of the Internet of Neurons and brainstorm about its disruptive impact, discussing the technological (and neurological) breakthroughs required to enable it, the new opportunities it provides and the security challenges it raises. We elaborate on the novel system models, threat models and security properties that are required to reason about privacy, security and trust in the Internet of Neurons. In doing so, we refer to aired Black Mirror episodes and possible new ones.

We proceed as follows. In Section II, we introduce the Internet of Neurons. In Section III, we discuss privacy, security and trust issues in the Internet of Neurons. In Section IV, we draw conclusions.

II. The Internet of Neurons: From brainwaves to packets, and vice versa

> *We are all now connected by the Internet, like neurons in a giant brain.* Stephen Hawking [14]

Although Hawking is famous for his predictions (as well as for his scientific results, of course), in this case he was not prophesying the advent of what we call the Internet of Neurons. However, it is interesting to note that he used the same keywords (we found this quote when we googled "Internet of Neurons" to see if somebody had already had the idea) and that, in a brain, like in the Internet, it is actually all a matter of connectivity.

How would connectivity work in the Internet of Neurons? At the root of all our thoughts, emotions and behaviors is the communication between neurons within our brains. *Brainwaves* are produced by synchronized electrical pulses from masses of neurons communicating with each other. Hence, to realize the *brain-net*, which is one of the frontiers of *brain-computer interaction* and thus of human-computer interaction, we need to interface brainwaves with the packets that are received and sent by computers or other external devices.[2]

Some approaches have already been proposed, and prototypical devices and software built, for the realization of *brain-computer interfaces* [15]. We can summarize the methodology behind brain-computer interaction, through a brain-computer interface, as the following sequence of steps:

1) Collect brainwaves by recording activity directly from the brain (invasively or non-invasively) in real-time.
2) Convert the complex waveforms of brainwaves into data.
3) Encode the parsed information and issue action instructions.
4) Feed back the externally perceived information in real-time in the form of signals that the brain can read (possibly through a stimulating device).

Note that the system must rely on intentional control, i.e., users must choose to perform a mental task whenever they want to accomplish a goal with the brain-computer interface.

Nowadays, it is already possible to detect and process brainwaves (e.g., using EEG sensors placed on the scalp) and a number of solutions have been proposed to provide a form of uni-directional communication and thus address at least steps 1) and 2) of this methodology. Let us consider three interesting examples. The neurotechnology company "Neuralink" was founded in 2016 by Elon Musk and others with the aim of developing an ultra-high-bandwidth implantable brain-computer interface to connect humans and computers [16]. While Neuralink is still in early stages, the "Brainternet" project [17] has developed an apparently more rudimentary but effective technology that streams brainwaves onto the Internet (by converting brainwaves into signals and streaming them to an online server using a Rasperry Pi computer). The startup "Neurable" created the VR game "Awakening" in which the gamer's brain essentially acts as mouse thanks to a brain-scanning headband paired with software that interprets the neural signals, thus allowing for hands-free control [18]. Other application areas that brain-computer interfaces are currently being developed for are, for instance, education (e.g., for monitoring of students' attention in real time) and medical care (e.g., for monitoring and treatment of Parkinson's and other serious brain diseases, with the eventual goal of human enhancement as aspired by Neuralink and other projects).

These technologies are promising, but they are still far from addressing steps 3) and 4) in a satisfactory way. The Internet of Neurons will require more than a uni-directional information flow; it will require a bi-directional information flow, in which

- brainwaves are translated into data and
- data is translated into signals that the brain can parse.

Some exploratory research is being carried out that attempts to bridge neuroscience with computer science and telecommu-

[2]Note that we are here assuming that the "normal" network will still be operating through packets, although by then advances in quantum computing (i.e., computing using quantum-mechanical phenomena, such as superposition and entanglement) might have provided for new modes of data transmission. But this is a topic for another paper.

nications, but brain-computer bi-directional information flow is still largely unchartered territory.

Nonetheless, we conjecture that by 2023, in five years from now[3], advances in neurology and in brain-computer interaction, combined with technological innovations, will have led to the creation of a device able to connect the human brain to the Internet bi-directionally, and without resorting to any invasive surgical operations.[4] This device won't be bulky; it will be portable, light and chargeable inductively so that we will be able to connect to the Internet anywhere anytime. It could take the form of a lightweight headphone like in Fig. 1 (and like in Black Mirror's "Playtest" (S03E02)) or more likely simply be a button-like pod that we will attach to our temples (like in Black Mirror's "San Junipero" (S03E04) and "USS Callister" (S04E07)). Or it could even be a tiny implant, although non-invasive procedures are typically to be preferred.

The device will communicate bidirectionally with the brain via brainwaves (as illustrated by the brainwave symbol on the forehead of the human in Fig. 1) and with the Internet via wireless communication (as illustrated by the standard symbol) to and from appropriate routers. The device must thus be capable of reading the brainwaves in real-time, more or less like EEG readers are capable of doing now, but it must also be capable of interpreting the brainwaves and transform them into their digital version, sending the coded version to the Internet. The device must also be capable of receiving incoming data, convert it into brainwaves (Step (3)) and send them to the brain (Step (4)).

Being able to convert data into brainwaves and vice versa is necessary in this phase. Progress in Machine Learning, AI and Big Data have made it possible to interpret brainwaves [20] mapping them with words or pictures creating a valid and applicable brainwaves-to-digital and digital-to-brainwaves codification. Feeding back the converted data into the brain requires techniques capable of stimulating the brain with signals. *Electroconvulsive therapy (ECT)*, *rapid transcranial magnetic stimulation (rTMS)* and *magnetic seizure therapy* are techniques able to deliver stimulation pulses through the tissue directly to the brain, even wirelessly [21], [22].

We also conjecture that advances in software and hardware will make sure that in 20 years or so there will be no more need for any wearable device to connect: as depicted in Fig. 2, humans will be able to connect to the Internet directly with their brainwaves, possibly through routers that "read" brainwaves remotely (say from a distance of a few meters like wireless routers do now with wireless signals), and transform the brainwaves into data and vice versa (i.e., brains downloading and uploading information from the network). This may sound like the killing argument of "tin-foil-hat conspiracy theorists", who wear hats made from one or more sheets of aluminum foil in the belief that the hat will shield the brain from threats such as electromagnetic fields, mind control, and mind reading. Although this could be the premise of several new Black Mirror episodes (e.g., based on the privacy, security and trust issues that we discuss below), this too is not really science fiction: research is ongoing on developing sensors that can be used to monitor the human electroencephalogram without electrical or physical contact with the body [23], [24], [25]. There is still a long way to go until these sensors are actually able to do more than just monitor but actually allow for the full realization of the four steps that we described above, but several foundation stones for the Internet of Neurons have been, or are in the process of being, laid so it is necessary that we start thinking about the privacy, security and trust challenges that will plague the Internet of Neurons. Some of these challenges will mirror the challenges that are plaguing Internet as we know it today, but other challenges will be novel and even more intriguing.

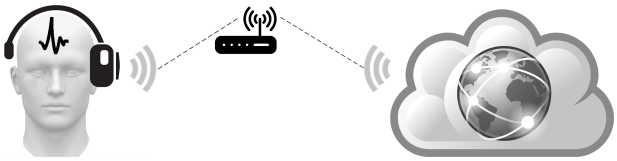

Fig. 1. Configuration 1 — Bi-directional brain-Internet connection by means of a wearable device

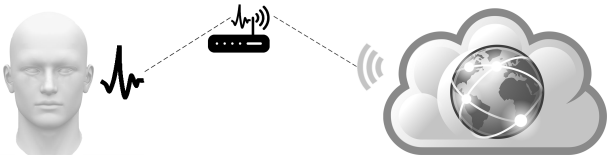

Fig. 2. Configuration 2 — Bi-directional brain-Internet direct connection

III. Privacy, security and trust

The potential offered by the technological revolution underlying the Internet of Neurons will be as varied as the problems related to privacy, security and trust that it will cause. In order to reason about these problems, we will need to provide suitable definitions, where a security definition is typically provided by combining a system model with a threat model and with one or more security properties that the system should guarantee even in the presence of an attacker. In the following, we discuss the main features of such models and properties for the Internet of Neurons. In our analysis, we thus take into account the two configurations suggested in the previous section, where the connection is made with or

[3]Actually, it is not really important whether it will be in 10, 20 or 30 years, but rather that this will happen for sure, in one form or the other. And this time we should do it right, considering security from the start, unlike what happened when Internet was first designed as pointed out Danny Hills in [19]:

> *Because the internet was designed for a community that trusted each other, it didn't have a lot of protections in it. We didn't worry about spying on each other, for example. We didn't worry about somebody sending out spam, or bad emails, or viruses, because such a person would have been banned from the community.*

[4]Implants are featured prominently in several Black Mirror episodes, e.g., "The Entire History of You" (S01E03), "White Christmas" (2014 special), "Nosedive" (S03E01), "Men Against Fire" (S03E05) and "Arkangel" (S05E05). These are all invasive implants that cannot be easily removed, thereby causing all sorts of problems to the people that "wear" them and to their families and friends.

without a device, pointing out analogies with, and differences from, current research and technologies.

A. System model

To provide a model of the system means to give a clear, and preferably formal, definition that provides enough detail to be able to understand and specify how the system behaves, encompassing both when it behaves correctly and securely, and when it behaves in unexpected and insecure ways.

In the security literature, security models have been formulated in a number of different ways. For instance, encryption and decryption operators are typically described by means of mathematical formulas along with some algebraic structure to capture the operators' properties; security protocols are typically described by means of state transition systems that specify how the knowledge of the protocol agents evolves over time; firewalls are typically described by means of sets of rules regulating how packets are filtered; access control systems are typically described by means of security policies, requests and permissions; software systems are typically described directly by their source code (or by the specification that can be learned or inferred by interacting with the code) or by dataflow and/or control flow specifications. These are just some examples, but all of them have in common the need to represent the infrastructure and how information flows among the system's agents (a.k.a. principals or entities).

For example, for Configuration 1 (Fig. 1), we can identify the following agents:

- the human being,
- the device,
- the router(s),
- the Internet,

connected by the following communication channels:

- a short-range channel between human being and device,
- a medium-range channel between device and router,
- a long-range (and possibly wired) channel between router and Internet.

Different protocols will be used to transmit information over these channels. The channel between the device and the router and the channel between the router and the Internet might actually employ protocols similar to the wireless protocols that we are already using today — in fact, if we are interested in a formal analysis of the system, we could even abstract away the channel between the router and the Internet and simply consider a medium–to-long-range channel between device and Internet. The channel between the human being and the device will, however, require new protocols able to translate between brainwaves and data packets, as the technologies that we discussed in the previous section are attempting to do.

For Configuration 2 (Fig. 2), we can identify the following agents:

- the human being,
- the router(s),
- the Internet,

connected by the following communication channels:

- a medium-range channel between human being and router,
- a long-range (and possibly wired) channel between router and Internet.

As before, different protocols will be used to transmit information over these channels. We expect that it will be possible to generalize to this configuration the protocols developed for the short-range brain-device communication in Configuration 1.

In both cases, the model of the configuration will need to be extended with models of the agents (including their actions and their states), of the security protocols used (including routing protocols), of the messages being sent, of the cryptography used and so on. We expect that many of the modeling languages and techniques that are in use today will be applicable with reasonable extensions, except of course for the translation brainwave-data, which will require considerable work. A starting point could be the formalization of this translation as a new cryptographic operator that encodes brainwaves into data along with the inverse operator that decodes data into brainwaves; identifying and formalizing the properties of these operators won't be easy though.

B. Threat model

A number of questions need to be answered in order to provide a threat model:

- *Who is the attacker?* Is he an outsider or an insider? Is he an agent (a human or a machine) trying to attack the communication between the human and the Internet? Is he perhaps the router, or even the human itself? What if the human behaves honestly but makes mistakes, or thinks "wrong thoughts" (whatever they may be) that make the system vulnerable? How would social engineering look like in this case?
- *Where is the attacker?* For instance, can the attacker attack all communication channels in the two configurations as in Fig.s 3 and 4? Or can we assume that the system contains a trusted network area? For example, Fig. 5 assumes that the short-range channel between brain and device cannot be attacked, perhaps supposing that the device itself is able to provide a kind of shield creating some "noise" that isolates the human brain and prevents remote reading (and writing) of brainwaves, like noise-cancellation headphones do with the urban noise. Another approach could be to establish some kind of "encryption" between brain and device, mapping device signals to a specific person's individual brainwaves. Alternatively, a more radical way would be to "implant" the device preventing possible substitutions with tampered devices. Other approaches could be possible. This situation is similar to the assumptions that are currently often made when reasoning about the security of complex security protocols (such as those built by composing subprotocols) [26], [27], [28] or of cyber-physical systems [29], where the attacker can only tamper with some, but not all, channels and devices. We thus expect that these recent works will be particularly useful.

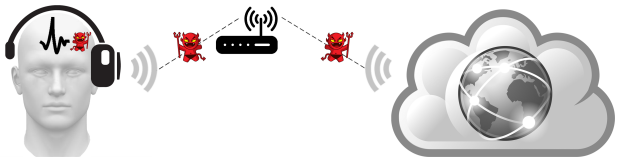

Fig. 3. Possible attacker locations in Configuration 1

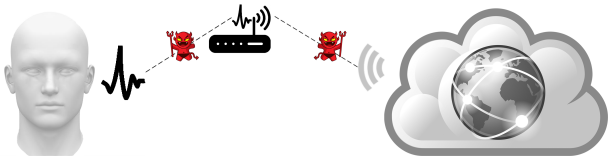

Fig. 4. Possible attacker locations in Configuration 2

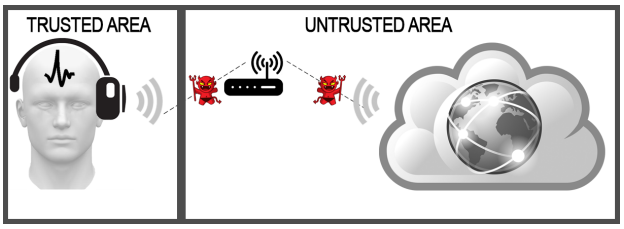

Fig. 5. Trusted area in Configuration 1

- *What is the power of the attacker?* What are his computational resources? Does he possess a certain amount of computation time to devote to his attack? Does he possess, or control, devices that allow him to access the different channels and the messages sent on them? Or perhaps should we assume that the attacker can inject some malicious code in the device or the router? In that way, he could not only do harm to the system or even spoof a router to gain access to the human brain, but perhaps also physical harm to the human, by tampering with the device that has direct access to the brain. The attacker could also spoof another human to gain access to a router. We will return to this when we discuss security properties in the next subsection. In fact, we must also answer the question: *What is the attacker trying to achieve?* What can he do on the different channels? Read, replace, modify, intercept messages and perhaps even brainwaves? To that end, we need to consider the security properties that the system is trying to achieve.

C. Properties

Let us now discuss the main security properties that we could ask the Internet of Neurons to guarantee. Note that although we focus on the traditional security properties, it is obvious that the categorical imperative of the Internet of Neurons is actually the *safety* of the human being, i.e.,

no harm should occur to the (brain of the) human being.

The Internet is already putting human safety at risk in several ways nowadays [30], [31], [32], but in the Internet of Neurons failure to guarantee one or more security properties (e.g., consequences of the Internet "tampering" directly the human brain) might actually expose, directly or indirectly, humans to novel and much more dangerous risks.

1) Privacy, Confidentiality and Authentication: Information privacy (a.k.a. *data privacy*) is the relationship between the collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. *Internet privacy* is a subset of information privacy that concerns the storing, repurposing, provision to third parties, and displaying of information pertaining to oneself by means of the Internet. In the Internet of Neurons, our "persona" is using one of the most private information we have: our thoughts, represented by brainwaves.

Thoughts and emotions are intrinsically and intricately related. In psychology, emotions are described as unconscious feelings that are the result of mostly unconscious thoughts [33]. A number of works have been published on how to extract human emotions from brainwaves using electroencephalography (EEG) [34], [35], [36], [37]. What would happen if the attacker were able to extract our emotions from the brainwaves that we are sending in the Internet of Neurons? How can we protect them from being stolen?

In Configuration 1 (as shown in Fig. 3), the attacker could intercept the brainwaves received by the device before they are coded and transmitted to the router and then the network. A study carried out in 2011 demonstrated technologies able to reconstruct images from brainwaves [38], so that, also thanks to some spoofing techniques, the attacker could intercept our communication, reverse it into brainwaves and thus obtain the raw data of our thoughts, even in their binary version. This hypothesis becomes even stronger if we consider a device-less configuration (as shown in Fig. 4) where there is no encoding of brainwaves and they are broadcast over the air to the Internet. This is reminiscent of the attacks that can be carried out by eavesdropping from a distance on the sound emanated by different keyboard keys [39], [40] or by eavesdropping from a distance on the data that is displayed on a computer screen [41]. In these two kinds of attacks, the attacker learns how to recognize and reconstruct the sound or image generated. We expect that advances in machine learning, coupled with those in neuroscience and brainwave-data translation, will make brainwave eavesdropping and reconstruction possible with affordable attacking devices.

Another major issue concerns *location privacy*. Several indoor and outdoor location techniques can be used to trace our position [42], [43], which can have positive or negative consequences. For instance, in 2011, the Chinese government announced that it would track people's movements through their cell phones for better traffic control [44], [45], while a study of the Haitian population after the 2010 earthquake showed that similar tracking is extremely useful in informing where people are and where relief aid should go [46]. The Internet of Neurons won't be exempt from mass surveillance issues, allowing attackers, including governments or Internet providers, to violate the users' location privacy.

We could assume that every brainwave-data device will have a unique identifier like most of the devices have, such as a uuid [47] or a global identifier that is created when the device accesses some services [48]. Tracking these identifiers will be possible, e.g., along the lines of [49]. Removing the device (and its identifier) as is done in Configuration 2, will help mitigate these problems, but still it won't guarantee location privacy. Recent studies [50], [51], [52] have namely shown that it is possible to create brainwave patterns to identify users, and thus use *brainprinting* as a biometric *authentication* factor.[5] In both of the configurations that we considered, with or without a device, the attacker could then track a specific user relying just on her brainprint. To that end, the attacker would, of course, need to know the user's brainprint, but, mimicking how authentication is done today, we could imagine a sort of brainprint certificate issued by a certification authority of a public-brainprint infrastructure[6], or we could simply consider the Internet or the Internet provider as the attacker able to track the movement of its users.

In this case, in order to attempt to achieve location privacy, users should try to change their brainprint. One way to alter one's thought pattern would be to learn to think differently than usual, e.g., thinking "happy thoughts" that obfuscate the normal pattern. This sounds a bit "mystical", but maybe one could indeed learn to confuse one's own brainwaves while still functioning normally as a human being. Alcohol and drugs might help here (although it might then be difficult to remember one's password [55]) or also physical exercise, workout, fatigue, hunger and stress, which all have been shown to alter one's EEG [56].

Another solution for privacy and location privacy, as well as for confidentiality, would be to encrypt. However, while we could use standard encryption algorithms (such as RSA, Triple DES or AES) to encrypt the wireless communication from device to router and from router to Internet, it is at best unclear how to encrypt the actual brainwaves, which are transmitted from brain to device in Configuration 1 or broadcast over the air in Configuration 2. But maybe one day somebody will devise an algorithm that allows humans to carry out mental encryption much in the same way as one can learn how to carry out mental calculations.

The device of Configuration 1 could raise other privacy questions. For instance, it could determine health-related issues while it is reading the user's brainwaves and provide, or sell, such information to health-insurance companies or the government. Could it also determine the user's emotions and thoughts? Will the user trust the device? How could we protect information that we know (e.g., passwords or other confidential data) from being read and distributed by the device? One could, similar to "happy thoughts" above, try to suppress one's thoughts about such confidential information when wearing the device, but this will be difficult if not impossible.[7] Or one could learn to store some thoughts in *private mental drawers*, like some mentalists are (supposedly) able to do. In any case, to ensure that users will trust the device, it will at the very least be necessary to carry out a strict procedure of testing and certification of the device before it is deployed. Similar comments apply also for Configuration 2, but referring to the router rather than to the wearable device.

2) Integrity: What does integrity mean in the Internet of Neurons? How can we protect thoughts and brainwaves? The attacker will attempt to tamper with all communication channels, the digital and the mental ones. In the case of digital channels (from device to router or from router to the network), we will likely be able to use integrity-preserving solutions similar to the ones that are available now (cryptographic checksums, hash functions, message authentication codes, digital signatures, and so on).[8]

There is of course also the question of the integrity of the human mind itself, i.e., protecting the brain from "malicious brainwaves" generated from malicious data from the network. In this case, we will need techniques for mental firewalls, input sanitization, sandboxing or Chinese-walling, thereby ensuring the security of the information contained in the other parts of the brain.

3) Availability: Besides for malfunctioning of the device and the router, and of jamming of the wireless signals, availability in the Internet of Neurons can be threatened by a *Distributed Denial of Service (DDoS)* attack when the brain is overwhelmed by the amount of incoming information, thus putting the human at risk. Filtering mechanisms will be necessary to control the flow of data.

On the other hand, the Internet of Neurons will enable opportunities that are unthinkable now. For instance, studies about sleep-learning [58], [59], [60], [61] have shown that our mind is able to learn if it is stimulated during the night under certain conditions. The Internet of Neurons would enable us to learn while we are sleeping thanks to the direct connection of our brain to the Internet. Actually, we could be learning in every waking moment, committing part of our brain to learning and leaving the remaining part untouched for everyday operations, i.e., for our brain's normal daily activity. We could even commit part of our brain as a CPU, e.g.,

[5]Other studies [53], [54] have investigated *pass-thought authentication*, which allows users to submit both a knowledge factor (i.e., a secret thought) and an inherence factor (i.e., the unique way that thought is expressed) in a single step, by performing a single mental task.

[6]The process behind the brainwave authentication methods that have been proposed requires the registration of a brainwave pattern: a sequence of images or a sequence of words are shown to a user and her brainwaves are stored as her brainprint. This process has to be done in exactly the same way for each user in order to obtain an impartial brainprint. Through this brainprint, an authentication system is able to recognize a user and then, if desired, to authenticate her requests. Note that in Configuration 1 we will also need to authenticate, and protect, the pairing of brain and device.

[7]This is reminiscent of the *paradox of thought suppression* [57], which originates from a challenge that Fyodor Dostoevsky posed in his 1863 essay "Winter Notes on Summer Impressions": *Try to pose for yourself this task: not to think of a polar bear, and you will see that the cursed thing will come to mind every minute*.

[8]In the case of analog channels and signals (from the device to the brain or from the brain to the router), integrity of analog brainwaves could be evaluated in the same way in which we recognize a friend's voice: first by recognition of familiar analog speech sounds, then by recognition of familiar linguistic patterns, and eventually by recognition of familiar behavioral cues and, if needed, through private shared history.

for mining and other cryptographic calculations, as we have imagined in [62].

4) Anonymity: One way to achieve at least some degree of anonymity in today's Internet is to use an anonymizing service (such as Mixes, I2P or TOR) that addresses the issue of IP tracking [63], [64] by encrypting packets within multiple layers of encryption. Anonymity is achievable because, as the packet follows a predetermined route through the anonymizing network, each router sees the previous router as the origin and the next router as the destination, and no router knows both the true origin and the true destination of the packet.

In Configuration 1 of the Internet of Neurons, some of the nodes of the network are actually other users with their devices, whereas other nodes are classic nodes like routers, computers and so on. In this case, the device could negotiate a preemptive path passing through a number of other devices creating a sort of onion routing. However, this kind of solution might not be applicable in Configuration 2 because it is unclear who would actually negotiate a route and apply multiple layers of encryption, unless we assume that brains are able to connect directly with each other, which is something that we will discuss in a bit more detail as we draw our conclusions.

IV. Conclusions

The premise of this paper is that in the near future the human brain will be at the center of a new Internet paradigm that we call Internet of Neurons. Some parts of our paper are deliberately science fiction (in the style of Black Mirror or other futuristic series and movies), but actually, as we have shown by means of the many ongoing works that we discussed, the seeds of the Internet of Neurons are already present in several of the technologies that are being used today or are under development. The opportunities will be prodigious, but repercussions for privacy, security and trust will be enormous and, frankly, tremendously scary (and we expect that they will inspire the Black Mirror writers). We have tried to dissect some of those challenges that researchers will have to face once this is all real (and trust us, it will become real in one form or the other), but we have only skimmed the surface.

More work is needed to fully understand and reason about system and threat models and security properties, specifying the ones we discussed above in more detail but also considering other properties that could be relevant for the Internet of Neurons. Moreover, we have made the quite strong assumption that brainwaves will need to be translated to data (and vice versa) as the Internet will still transmit packets. But by, say, 2050, it could well be that the network will follow a radically different model, perhaps thanks to advances in quantum computing or in "brainwave computing" (a discipline that we just invented), allowing the network to directly process brainwaves as shown in Fig. 6. But why stop here? If brainwave transmission protocols are possible, then it means that the network is able to read the brainwaves that a brain is emanating, but also that the brain is able to receive brainwaves in input. How long will it then take before we find a way for brains to connect not only to the network but also to each other? Some research in this direction is already ongoing [65], [66] and the ultimate Internet of Neurons might then simply be based on direct brain-brain connections as the one in Fig. 7.

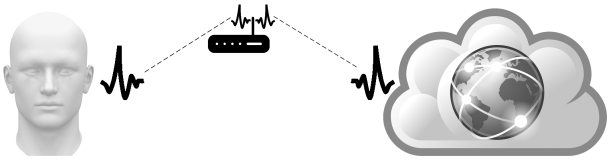

Fig. 6. Bi-directional brain-Internet connection by means of brainwaves

Fig. 7. Bi-directional brain-brain direct connection

Finally, there is an elephant in the room that we have not addressed in this paper. In addition to technological and neurological questions, some of which we discussed above, there are a huge number of economical, political and ethical issues that we don't really feel competent to address, but that will have to be tackled before we open our mind to the Internet. Who will pay for the Internet of Neurons? Will all citizens be taxed? Will governments or perhaps corporations provide it for free? Given that nothing is actually free, what will they want in return? In the wake of the recent scandals on data collection (such as the Facebook–Cambridge Analytica data scandal that involved the collection of personally identifiable information of up to 87 million Facebook users), we are skeptical that the Internet of Neurons will be exempt from massive personal data collection and mining, possibly opening up the possibility for big-brother scenarios in which citizens are always observed and tracked in order to control and influence their thoughts, opinions, votes, in brief, their whole life.

References

[1] A. M. Turing, "Computing machinery and intelligence," *Mind*, vol. 59, pp. 433–460, 1950.

[2] M. L. Shetterly, *Hidden Figures: The Story of the African-American Women Who Helped Win the Space Race*. W. Morrow & Co., 2016.

[3] P. J. Denning, "The Science of Computing: The ARPANET after Twenty Years," *American Scientist*, vol. 77, no. 6, pp. 530–534, 1989.

[4] C. Schroth and T. Janner, "Web 2.0 and SOA: Converging Concepts Enabling The Internet Of Services," *IT professional*, vol. 9, no. 3, 2007.

[5] K. Mandula, R. Parupalli, C. A. Murty, E. Magesh, and R. Lunagariya, "Mobile based home automation using Internet of Things (IoT)," in *ICCICCT*. IEEE, 2015, pp. 340–343.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Commun. Surveys Tuts*, vol. 4, 2015.

[8] F. Osisanwo, S. Kuyoro, and O. Awodele, "Internet Refrigerator–A typical Internet of Things (IoT)," 2015.

[9] M. Simsek, A. Aijaz, M. Dohler, J. Sachs, and G. Fettweis, "5G-Enabled Tactile Internet," *J. Sel. Areas Commun.*, vol. 34, no. 3, 2016.

[10] S. Kavanagh. (2018) What is the Tactile Internet. [Online]. Available: https://5g.co.uk/guides/what-is-the-tactile-internet

[11] M. Dohler, T. Mahmoodi, M. A. Lema, M. Condoluci, F. Sardis, K. Antonakoglou, and H. Aghvami, "Internet of Skills, where Robotics meets AI, 5G and the Tactile Internet," in *EuCNC*, 2017, pp. 1–5.

[12] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5g security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.

[13] P. Schneider and G. Horn, "Towards 5g security," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, vol. 1. IEEE, 2015, pp. 1165–1170.

[14] USA Today. (2014) Q&A with Stephen Hawking. [Online]. Available: https://www.usatoday.com/story/tech/2014/12/02/stephen-hawking-intel-technology/18027597/

[15] B. Graimann, B. Allison, and G. Pfurtscheller, "Brain-Computer Interfaces: A Gentle Introduction," pp. 1–27, 2010.

[16] R. Winkler, "Elon Musk Launches Neuralink to Connect Brains With Computers," *Wall Street Journal. https://www. wsj. com*, 2017.

[17] D. Minors. (2017) Can you read my mind? [Online]. Available: https://www.wits.ac.za/news/latest-news/research-news/2017/2017-09/can-you-read-my-mind

[18] E. Strickland, "Mind games," *IEEE Spectrum*, vol. 55, no. 1, 2018.

[19] W. Herzog (directed by). (2016) Lo and Behold, Reveries of the Connected World. https://www.imdb.com/title/tt5275828/.

[20] H. Wen, J. Shi, Y. Zhang, K.-H. Lu, J. Cao, and Z. Liu, "Neural encoding and decoding with deep learning for dynamic natural vision," *Cerebral Cortex*, pp. 1–25, 2017.

[21] R. Chen, G. Romero, M. G. Christiansen, A. Mohr, and P. Anikeeva, "Wireless magnetothermal deep brain stimulation," *Science*, 2015.

[22] N. Grossman, D. Bono, N. Dedic, S. B. Kodandaramaiah, A. Rudenko, H.-J. Suk, A. M. Cassara, E. Neufeld, N. Kuster, L.-H. Tsai *et al.*, "Noninvasive deep brain stimulation via temporally interfering electric fields," *Cell*, vol. 169, no. 6, pp. 1029–1041, 2017.

[23] C. Harland, T. Clark, and R. Prance, "Remote detection of human electroencephalograms using ultrahigh input impedance electric potential sensors," *Appl. Phys. Lett.*, vol. 81, pp. 3284–3286, 2002.

[24] R. Prance, S. T. Beardsmore-Rust, P. Watson, C. Harland, and H. Prance, "Remote detection of human electrophysiological signals using electric potential sensors," *Applied Physics Letters*, vol. 93, no. 3, 2008.

[25] E. Rendon Morales, R. Prance, H. Prance, and R. Aviles-Espinosa, "A novel non-invasive biosensor based on electric field detection for cardio-electrophysiology in zebrafish embryos," *Procedia Technology*, vol. 24, pp. 242–243, 2017.

[26] O. Almousa, S. Mödersheim, P. Modesti, and L. Viganò, "Typing and Compositionality for Security Protocols: A Generalization to the Geometric Fragment," in *ESORICS*, ser. LNCS 9327. Springer, 2015, pp. 209–229.

[27] S. Mödersheim and L. Viganò, "Sufficient conditions for vertical composition of security protocols," in *ASIACCS*. ACM, 2014, pp. 435–446.

[28] ——, "Secure Pseudonymous Channels," in *ESORICS*, ser. LNCS 5789. Springer, 2009, pp. 337–354.

[29] R. Lanotte, M. Merro, R. Muradore, and L. Viganò, "A Formal Approach to Cyber-Physical Attacks," in *CSF*. IEEE, 2017, pp. 436–450.

[30] R. Kiley, "Does the internet harm health?: Some evidence exists that the internet does harm health," *British Medical Journal*, vol. 324, 2002.

[31] D. J. Kuss, M. D. Griffiths, and J. F. Binder, "Internet addiction in students: Prevalence and risk factors," *Comput Human Behav*, vol. 29, no. 3, 2013.

[32] Y. S. Lee, D. H. Han, S. M. Kim, and P. F. Renshaw, "Substance abuse precedes internet addiction," *Addictive behaviors*, vol. 38, 2013.

[33] M. Pettinelli, *The psychology of emotions, feelings and thoughts*. Connexions, 2011.

[34] W. Wan Ismail, M. Hanif, S. Mohamed, N. Hamzah, and Z. I. Rizman, "Human emotion detection via brain waves study by using electroencephalogram (EEG)," *IJASEIT*, vol. 6, no. 6, 2016.

[35] F.-C. Kao, S. P. Wang, and Y.-J. Chang, "Brainwaves analysis of positive and negative emotions," *ISAA,(12)*, pp. 1263–1266, 2015.

[36] P. Lahane and A. K. Sangaiah, "An approach to eeg based emotion recognition and classification using kernel density estimation," *Procedia Computer Science*, vol. 48, pp. 574–581, 2015.

[37] T. Y. Chai, S. S. Woo, M. Rizon, and C. S. Tan, "Classification of human emotions from eeg signals using statistical features and neural network," in *International*, vol. 1, no. 3. Penerbit UTHM, 2010, pp. 1–6.

[38] Berkley News, Yasmin Anwar, Media Relations. (2011) Scientists use brain imaging to reveal the movies in our mind. [Online]. Available: http://news.berkeley.edu/2011/09/22/brain-movies/

[39] D. Asonov and R. Agrawal, "Keyboard acoustic emanations," in *IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2004, pp. 3–11.

[40] L. Zhuang, F. Zhou, and J. Tygar, "Keyboard Acoustic Emanations Revisited," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, pp. 1–26, 2009.

[41] M. Backes, M. Dürmuth, and D. Unruh, "Compromising Reflections-or-How to Read LCD Monitors around the Corner," in *IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2008, pp. 158–169.

[42] C. Benavente-Peces, M. Puente, A. Domínguez-García, M. Lugilde-Rodríguez, E. de la Serna, D. Miguel, and A. García, "Global System for Localization and Guidance of Dependant People: Indoor and Outdoor Technologies Integration," in *Ambient Assistive Health and Wellness Management in the Heart of the City*. Springer, 2009, pp. 82–89.

[43] M. Werner, "Basic positioning techniques," in *Indoor Location-Based Services*. Springer, 2014, pp. 73–99.

[44] Tania Branigan. (2011) China plans to track beijing citizens through their mobiles. [Online]. Available: https://www.theguardian.com/world/2011/mar/04/china-tracking-beijing-citizens-mobiles

[45] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, "Privacy and cybersecurity: The next 100 years," *Proceedings of the IEEE*, vol. 100, pp. 1659–1673, 2012.

[46] L. Bengtsson, X. Lu, A. Thorson, R. Garfield, and J. Von Schreeb, "Improved response to disasters and outbreaks by tracking population movements with mobile phone network data: a post-earthquake geospatial study in Haiti," *PLoS medicine*, vol. 8, no. 8, 2011.

[47] P. J. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) urn namespace," 2005.

[48] A. R. Jones, E. E. L. Quah, D. J. Nielsen, and L. Eminovic, "Creating a globally unique identifier of a subscriber device," 2012, US Patent 8,213,935.

[49] S. Koneru and M. H. Tuchen, "Tracking a user across both secure and non-secure areas on the internet, wherein the users is initially tracked using a globally unique identifier," Oct. 12 1999, uS Patent 5,966,705.

[50] B. C. Armstrong, M. V. Ruiz-Blondet, N. Khalifian, K. J. Kurtz, Z. Jin, and S. Laszlo, "Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for erp biometrics," *Neurocomputing*, vol. 166, pp. 59–67, 2015.

[51] P. Kumari and A. Vaish, "Brainwave based authentication system: research issues and challenges," *Int J Comput Appl*, vol. 4, no. 1, 2014.

[52] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, "Cerebre: A novel method for very high accuracy event-related potential biometric identification," *IEEE Trans. Inf. Forensic Secur.*, vol. 11, no. 7, 2016.

[53] J. Thorpe, P. C. van Oorschot, and A. Somayaji, "Pass-thoughts: authenticating with our minds," in *NSPW*. ACM, 2005, pp. 45–56.

[54] N. Merrill, M. T. Curran, and J. Chuang, "Is the Future of Authenticity All In Our Heads?: Moving Passthoughts From the Lab to the World," in *NSPW*. ACM, 2017, pp. 70–79.

[55] N. Kobie, "Brainwaves could act as your password — but not if you're drunk," *New Scientist*, 2017.

[56] G. Chuang and J. Chuang, "Passthoughts on the Go: Effect of Exercise on EEG Authentication (Extended Version)," 2016.

[57] D. M. Wegner, *White Bears and Other Unwanted Thoughts: Suppression, Obsession, and the Psychology of Mental Control*. The Guilford Press, 1994.

[58] C. W. Simon and W. H. Emmons, "Learning during sleep?" *Psychological Bulletin*, vol. 52, no. 4, p. 328, 1955.

[59] J. D. Rudoy, J. L. Voss, C. E. Westerberg, and K. A. Paller, "Strengthening individual memories by reactivating them during sleep," *Science*, vol. 326, no. 5956, pp. 1079–1079, 2009.

[60] J. W. Antony, E. W. Gobel, J. K. O'hare, P. J. Reber, and K. A. Paller, "Cued memory reactivation during sleep influences skill learning," *Nature neuroscience*, vol. 15, no. 8, p. 1114, 2012.

[61] A. Arzi, L. Shedlesky, M. Ben-Shaul, K. Nasser, A. Oksenberg, I. S. Hairston, and N. Sobel, "Humans can learn new information during sleep," *Nature neuroscience*, vol. 15, no. 10, p. 1460, 2012.

[62] D. Sempreboni and L. Viganò, "May I Mine Your Mind?" in *2nd ReCoding Black Mirror workshop, Companion of The Web Conference (WWW)*. ACM, 2018, pp. 1573–1576.

[63] B. Zantout and R. Haraty, "I2p data communication system," in *Proceedings of ICN*. Citeseer, 2011, pp. 401–409.

[64] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, "Anonymous connections and onion routing," *J. Sel. Areas Commun.*, vol. 16, 1998.
[65] C. Grau, R. Ginhoux, A. Riera, T. L. Nguyen, H. Chauvat, M. Berg, J. L. Amengual, A. Pascual-Leone, and G. Ruffini, "Conscious brain-to-brain communication in humans using non-invasive technologies," *PLoS One*, vol. 9, no. 8, 2014.
[66] R. P. Rao, A. Stocco, M. Bryan, D. Sarma, T. M. Youngquist, J. Wu, and C. S. Prat, "A Direct Brain-to-Brain Interface in Humans," *PLoS One*, vol. 9, no. 11, pp. 1–12, 11 2014.